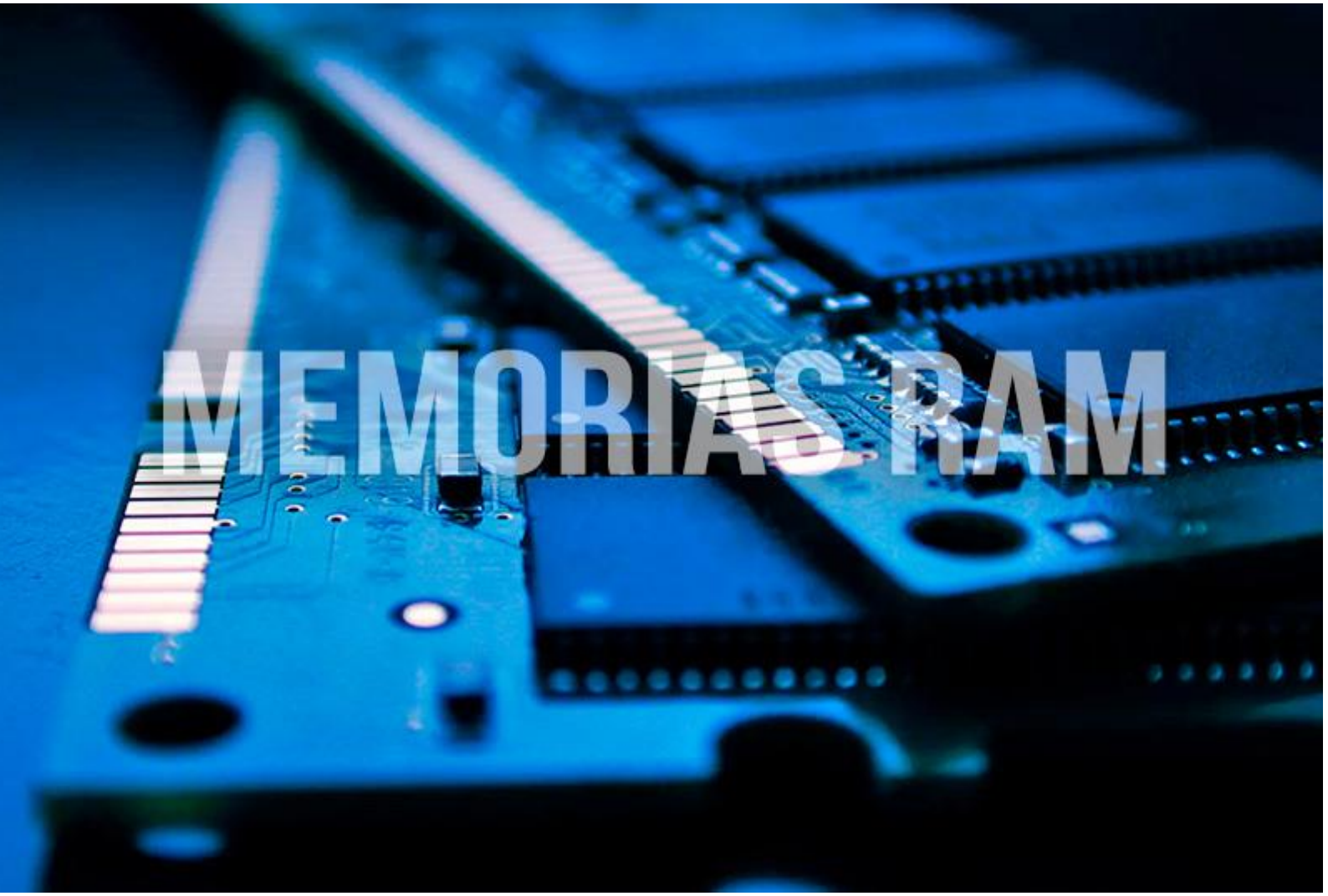


Fray José Ávila Hernández

ÍNDICE

1.Adquisición de memoria ram

```
C:\Herramientas>winpmem_mini_x64_rc2.exe windows_ram.mem
WinPmem64
Extracting driver to C:\Users\forensic\AppData\Local\Temp\pmeBEB1.tmp
Driver Unloaded.
Loaded Driver C:\Users\forensic\AppData\Local\Temp\pmeBEB1.tmp.
Deleting C:\Users\forensic\AppData\Local\Temp\pmeBEB1.tmp
The system time is: 19:25:35
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AA000
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xDFEED000
Start 0x100000000 - Length 0x5F300000
max_physical_memory_ 0x15f300000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000

00% 0x00000000 .
copy_memory
 - start: 0x1000
 - end: 0x9f000

00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
pad
 - length: 0x61000

00% 0x0009F000 .
copy_memory
 - start: 0x100000
 - end: 0x102000

00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
pad
 - length: 0x1000

00% 0x00102000 .
copy_memory
 - start: 0x103000
 - end: 0xdfff0000

00% 0x00103000 ..................................................
14% 0x32103000 ..................................................
28% 0x64103000 ..................................................
42% 0x96103000 ..................................................
56% 0xC8103000 ..........................
Padding from 0xDFFF0000 to 0x100000000
pad
 - length: 0x20010000

63% 0xDFFF0000 ................................
copy_memory
 - start: 0x100000000
 - end: 0x15f300000

72% 0x100000000 ..................................................
87% 0x132000000 ..............................................
The system time is: 19:29:24
Driver Unloaded.
```

La máquina a la que vamos a extraer la memoria ram es una máquina virtual cuyo sistema operativo es Windows 10.

Para la adquisición hemos utilizado la herramienta ***"winpmem_mini_x64_rc2.exe"*** con el siguiente comando:

"C:\Herramientas> winpmem_mini_x64_rc2.exe windows_ram.mem" que lo que ha hecho es guardarnos una copia de la memoria en el archivo (imagen) que hemos denominado ***"Windows_ram.mem"***

```
C:\Users\forensic>ping google.es

Haciendo ping a google.es [142.250.184.3] con 32 bytes de datos:
Respuesta desde 142.250.184.3: bytes=32 tiempo=14ms TTL=116
Respuesta desde 142.250.184.3: bytes=32 tiempo=12ms TTL=116
Respuesta desde 142.250.184.3: bytes=32 tiempo=21ms TTL=116
Respuesta desde 142.250.184.3: bytes=32 tiempo=12ms TTL=116

Estadísticas de ping para 142.250.184.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 12ms, Máximo = 21ms, Media = 14ms
```

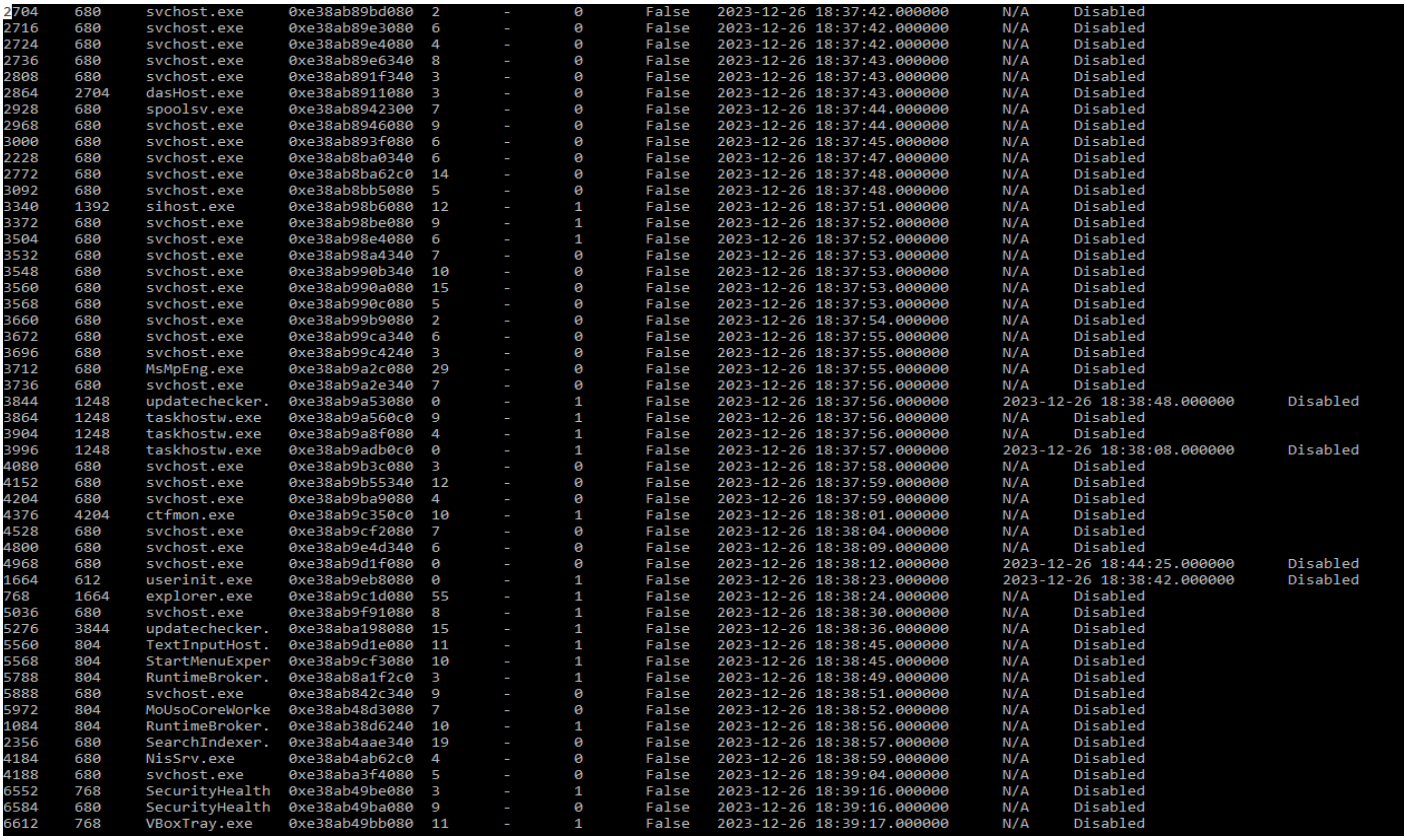
Cuando hemos ejecutado la herramienta ***"Winpmem_mini_x64_rx2.exe"*** hemos lanzado también un ping al dominio de "Google.es" para que lo captara también a la hora de adquirir la memoria ram.

2.Volatility

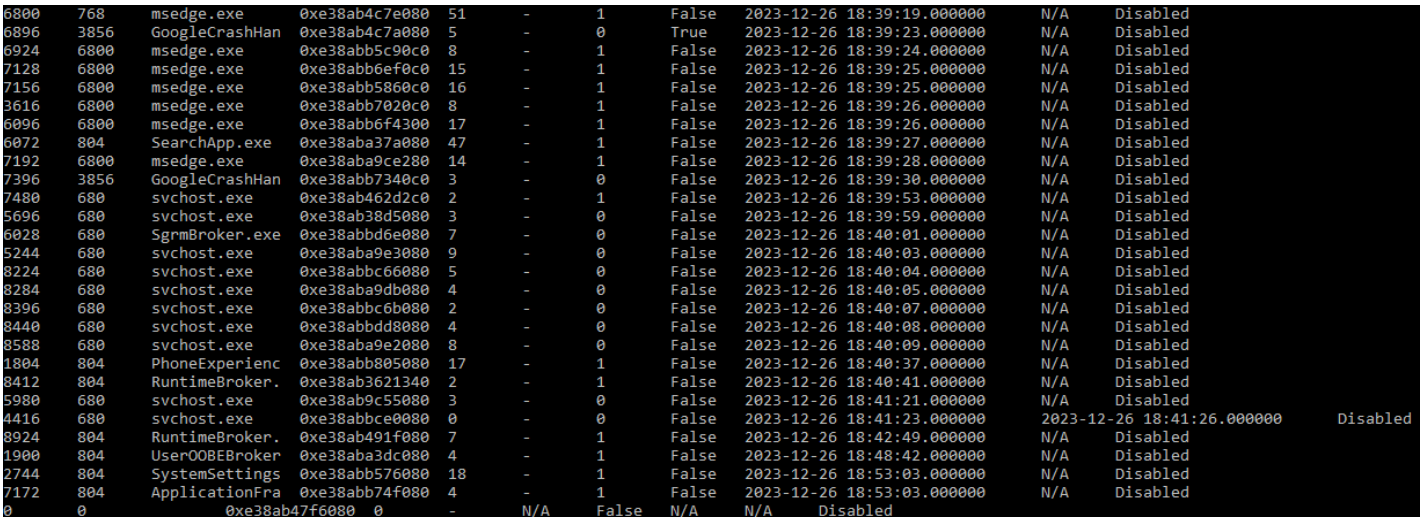
2.1 Windows.pslist.PsList

```
C:\Herramientas\volatility3-2.4.0\volatility3-2.4.0>python vol.py -f C:\Herramientas\windows_ram.mem windows.pslist.PsList
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File outp

4       0       System  0xe38ab1e83040  127     -       N/A     False   2023-12-26 18:37:01.000000      N/A     Disabled
92      4       Registry        0xe38ab1fba040  4       -       N/A     False   2023-12-26 18:36:34.000000      N/A     Disabled
348     4       smss.exe        0xe38ab3e7f040  2       -       N/A     False   2023-12-26 18:37:01.000000      N/A     Disabled
460     448     csrss.exe       0xe38ab4f0b080  11      -       0       False   2023-12-26 18:37:22.000000      N/A     Disabled
544     448     wininit.exe     0xe38ab4a80080  1       -       0       False   2023-12-26 18:37:24.000000      N/A     Disabled
552     536     csrss.exe       0xe38ab4a85140  12      -       1       False   2023-12-26 18:37:24.000000      N/A     Disabled
612     536     winlogon.exe    0xe38ab4555080  6       -       1       False   2023-12-26 18:37:24.000000      N/A     Disabled
680     544     services.exe    0xe38ab4a83140  10      -       0       False   2023-12-26 18:37:25.000000      N/A     Disabled
696     544     lsass.exe       0xe38ab4ca4080  12      -       0       False   2023-12-26 18:37:25.000000      N/A     Disabled
804     680     svchost.exe     0xe38ab873a340  15      -       0       False   2023-12-26 18:37:27.000000      N/A     Disabled
828     612     fontdrvhost.ex  0xe38ab8742240  5       -       1       False   2023-12-26 18:37:28.000000      N/A     Disabled
836     544     fontdrvhost.ex  0xe38ab8744240  5       -       0       False   2023-12-26 18:37:28.000000      N/A     Disabled
928     680     svchost.exe     0xe38ab4c09080  18      -       0       False   2023-12-26 18:37:28.000000      N/A     Disabled
980     680     svchost.exe     0xe38ab8224340  6       -       0       False   2023-12-26 18:37:28.000000      N/A     Disabled
720     680     svchost.exe     0xe38ab851d340  6       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1032    680     svchost.exe     0xe38ab85230c0  4       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1040    680     svchost.exe     0xe38ab852b080  3       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1056    680     svchost.exe     0xe38ab852a080  2       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1108    680     svchost.exe     0xe38ab854a080  4       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1228    680     svchost.exe     0xe38ab8581080  8       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1240    680     svchost.exe     0xe38ab8584340  5       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1248    680     svchost.exe     0xe38ab8587340  12      -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1332    680     svchost.exe     0xe38ab85b9080  5       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1340    680     svchost.exe     0xe38ab85bc0c0  5       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1392    680     svchost.exe     0xe38ab8621340  7       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1444    680     svchost.exe     0xe38ab8627080  7       -       0       False   2023-12-26 18:37:32.000000      N/A     Disabled
1516    680     svchost.exe     0xe38ab86780c0  3       -       0       False   2023-12-26 18:37:33.000000      N/A     Disabled
1584    680     svchost.exe     0xe38ab1e86080  6       -       0       False   2023-12-26 18:37:33.000000      N/A     Disabled
1688    680     svchost.exe     0xe38ab454d080  8       -       0       False   2023-12-26 18:37:34.000000      N/A     Disabled
1728    680     VBoxService.ex  0xe38ab86a3340  11      -       0       False   2023-12-26 18:37:35.000000      N/A     Disabled
1876    680     svchost.exe     0xe38ab8a22080  2       -       0       False   2023-12-26 18:37:35.000000      N/A     Disabled
1920    680     svchost.exe     0xe38ab8a7d080  5       -       0       False   2023-12-26 18:37:36.000000      N/A     Disabled
1928    680     svchost.exe     0xe38ab8a7f0c0  9       -       0       False   2023-12-26 18:37:36.000000      N/A     Disabled
1948    680     svchost.exe     0xe38ab8a8d340  4       -       0       False   2023-12-26 18:37:36.000000      N/A     Disabled
1964    680     svchost.exe     0xe38ab4fe30c0  10      -       0       False   2023-12-26 18:37:36.000000      N/A     Disabled
1408    4       MemCompression  0xe38ab8abd040  26      -       N/A     False   2023-12-26 18:37:37.000000      N/A     Disabled
1564    680     svchost.exe     0xe38ab8abf340  2       -       0       False   2023-12-26 18:37:37.000000      N/A     Disabled
2076    680     svchost.exe     0xe38ab8ac0080  3       -       0       False   2023-12-26 18:37:37.000000      N/A     Disabled
2140    680     svchost.exe     0xe38ab88720c0  6       -       0       False   2023-12-26 18:37:37.000000      N/A     Disabled
2148    680     svchost.exe     0xe38ab8877080  3       -       0       False   2023-12-26 18:37:37.000000      N/A     Disabled
2168    680     svchost.exe     0xe38ab887b0c0  2       -       0       False   2023-12-26 18:37:38.000000      N/A     Disabled
2216    680     svchost.exe     0xe38ab88830c0  11      -       0       False   2023-12-26 18:37:38.000000      N/A     Disabled
2336    680     svchost.exe     0xe38ab88a0080  5       -       0       False   2023-12-26 18:37:39.000000      N/A     Disabled
2464    680     svchost.exe     0xe38ab88e3340  14      -       0       False   2023-12-26 18:37:40.000000      N/A     Disabled
2584    680     svchost.exe     0xe38ab84a3080  11      -       0       False   2023-12-26 18:37:41.000000      N/A     Disabled
```



2704	680	svchost.exe	0xe38ab89bd080	2	-	0	False	2023-12-26 18:37:42.000000	N/A	Disabled
2716	680	svchost.exe	0xe38ab89e3080	6	-	0	False	2023-12-26 18:37:42.000000	N/A	Disabled
2724	680	svchost.exe	0xe38ab89e4080	4	-	0	False	2023-12-26 18:37:42.000000	N/A	Disabled
2736	680	svchost.exe	0xe38ab89e6340	8	-	0	False	2023-12-26 18:37:43.000000	N/A	Disabled
2808	680	svchost.exe	0xe38ab891f340	3	-	0	False	2023-12-26 18:37:43.000000	N/A	Disabled
2864	2704	dasHost.exe	0xe38ab8911080	3	-	0	False	2023-12-26 18:37:43.000000	N/A	Disabled
2928	680	spoolsv.exe	0xe38ab8942300	7	-	0	False	2023-12-26 18:37:44.000000	N/A	Disabled
2968	680	svchost.exe	0xe38ab8946080	9	-	0	False	2023-12-26 18:37:44.000000	N/A	Disabled
3000	680	svchost.exe	0xe38ab893f080	6	-	0	False	2023-12-26 18:37:45.000000	N/A	Disabled
2228	680	svchost.exe	0xe38ab8ba0340	6	-	0	False	2023-12-26 18:37:47.000000	N/A	Disabled
2772	680	svchost.exe	0xe38ab8ba62c0	14	-	0	False	2023-12-26 18:37:48.000000	N/A	Disabled
3092	680	svchost.exe	0xe38ab8bb5080	5	-	0	False	2023-12-26 18:37:48.000000	N/A	Disabled
3340	1392	sihost.exe	0xe38ab98b6080	12	-	1	False	2023-12-26 18:37:51.000000	N/A	Disabled
3372	680	svchost.exe	0xe38ab98be080	9	-	1	False	2023-12-26 18:37:52.000000	N/A	Disabled
3504	680	svchost.exe	0xe38ab98e4080	6	-	1	False	2023-12-26 18:37:52.000000	N/A	Disabled
3532	680	svchost.exe	0xe38ab98a4340	7	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3548	680	svchost.exe	0xe38ab990b340	10	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3560	680	svchost.exe	0xe38ab990a080	15	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3568	680	svchost.exe	0xe38ab990c080	5	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3660	680	svchost.exe	0xe38ab99b9080	2	-	0	False	2023-12-26 18:37:54.000000	N/A	Disabled
3672	680	svchost.exe	0xe38ab99ca340	6	-	0	False	2023-12-26 18:37:55.000000	N/A	Disabled
3696	680	svchost.exe	0xe38ab99c4240	3	-	0	False	2023-12-26 18:37:55.000000	N/A	Disabled
3712	680	MsMpEng.exe	0xe38ab9a2c080	29	-	0	False	2023-12-26 18:37:55.000000	N/A	Disabled
3736	680	svchost.exe	0xe38ab9a2e340	7	-	0	False	2023-12-26 18:37:56.000000	N/A	Disabled
3844	1248	updatechecker.	0xe38ab9a53080	0	-	1	False	2023-12-26 18:37:56.000000	2023-12-26 18:38:48.000000	Disabled
3864	1248	taskhostw.exe	0xe38ab9a560c0	9	-	1	False	2023-12-26 18:37:56.000000	N/A	Disabled
3904	1248	taskhostw.exe	0xe38ab9a8f080	4	-	1	False	2023-12-26 18:37:56.000000	N/A	Disabled
3996	1248	taskhostw.exe	0xe38ab9adb0c0	0	-	1	False	2023-12-26 18:37:57.000000	2023-12-26 18:38:08.000000	Disabled
4080	680	svchost.exe	0xe38ab9b3c080	3	-	0	False	2023-12-26 18:37:58.000000	N/A	Disabled
4152	680	svchost.exe	0xe38ab9b55340	12	-	0	False	2023-12-26 18:37:59.000000	N/A	Disabled
4204	680	svchost.exe	0xe38ab9ba9080	4	-	0	False	2023-12-26 18:37:59.000000	N/A	Disabled
4376	4204	ctfmon.exe	0xe38ab9c350c0	10	-	1	False	2023-12-26 18:38:01.000000	N/A	Disabled
4528	680	svchost.exe	0xe38ab9cf2080	7	-	0	False	2023-12-26 18:38:04.000000	N/A	Disabled
4800	680	svchost.exe	0xe38ab9e4d340	6	-	0	False	2023-12-26 18:38:09.000000	N/A	Disabled
4968	680	svchost.exe	0xe38ab9d1f080	0	-	0	False	2023-12-26 18:38:12.000000	2023-12-26 18:44:25.000000	Disabled
1664	612	userinit.exe	0xe38ab9eb8080	0	-	1	False	2023-12-26 18:38:23.000000	2023-12-26 18:38:42.000000	Disabled
768	1664	explorer.exe	0xe38ab9c1d080	55	-	1	False	2023-12-26 18:38:24.000000	N/A	Disabled
5036	680	svchost.exe	0xe38ab9f91080	8	-	1	False	2023-12-26 18:38:30.000000	N/A	Disabled
5276	3844	updatechecker.	0xe38aba198080	15	-	1	False	2023-12-26 18:38:36.000000	N/A	Disabled
5560	804	TextInputHost.	0xe38ab9d1e080	11	-	1	False	2023-12-26 18:38:45.000000	N/A	Disabled
5568	804	StartMenuExper	0xe38ab9cf3080	10	-	1	False	2023-12-26 18:38:45.000000	N/A	Disabled
5788	804	RuntimeBroker.	0xe38ab8a1f2c0	3	-	1	False	2023-12-26 18:38:49.000000	N/A	Disabled
5888	680	svchost.exe	0xe38ab842c340	9	-	0	False	2023-12-26 18:38:51.000000	N/A	Disabled
5972	804	MoUsoCoreWorke	0xe38ab48d3080	7	-	0	False	2023-12-26 18:38:52.000000	N/A	Disabled
1084	804	RuntimeBroker.	0xe38ab38d6240	10	-	1	False	2023-12-26 18:38:56.000000	N/A	Disabled
2356	680	SearchIndexer.	0xe38ab4aae340	19	-	0	False	2023-12-26 18:38:57.000000	N/A	Disabled
4184	680	NisSrv.exe	0xe38ab4ab62c0	4	-	0	False	2023-12-26 18:38:59.000000	N/A	Disabled
4188	680	svchost.exe	0xe38aba3f4080	5	-	0	False	2023-12-26 18:39:04.000000	N/A	Disabled
6552	768	SecurityHealth	0xe38ab49be080	3	-	1	False	2023-12-26 18:39:16.000000	N/A	Disabled
6584	680	SecurityHealth	0xe38ab49ba080	9	-	0	False	2023-12-26 18:39:16.000000	N/A	Disabled
6612	768	VBoxTray.exe	0xe38ab49bb080	11	-	1	False	2023-12-26 18:39:17.000000	N/A	Disabled



6800	768	msedge.exe	0xe38ab4c7e080	51	-	1	False	2023-12-26 18:39:19.000000	N/A	Disabled
6896	3856	GoogleCrashHan	0xe38ab4c7a080	5	-	0	True	2023-12-26 18:39:23.000000	N/A	Disabled
6924	6800	msedge.exe	0xe38abb5c90c0	8	-	1	False	2023-12-26 18:39:24.000000	N/A	Disabled
7128	6800	msedge.exe	0xe38abb6ef0c0	15	-	1	False	2023-12-26 18:39:25.000000	N/A	Disabled
7156	6800	msedge.exe	0xe38abb5860c0	16	-	1	False	2023-12-26 18:39:25.000000	N/A	Disabled
3616	6800	msedge.exe	0xe38abb7020c0	8	-	1	False	2023-12-26 18:39:26.000000	N/A	Disabled
6096	6800	msedge.exe	0xe38abb6f4300	17	-	1	False	2023-12-26 18:39:26.000000	N/A	Disabled
6072	804	SearchApp.exe	0xe38aba37a080	47	-	1	False	2023-12-26 18:39:27.000000	N/A	Disabled
7192	6800	msedge.exe	0xe38aba9ce280	14	-	1	False	2023-12-26 18:39:28.000000	N/A	Disabled
7396	3856	GoogleCrashHan	0xe38abb7340c0	3	-	0	False	2023-12-26 18:39:30.000000	N/A	Disabled
7480	680	svchost.exe	0xe38ab462d2c0	2	-	1	False	2023-12-26 18:39:53.000000	N/A	Disabled
5696	680	svchost.exe	0xe38ab38d5080	3	-	0	False	2023-12-26 18:39:59.000000	N/A	Disabled
6028	680	SgrmBroker.exe	0xe38abbd6e080	7	-	0	False	2023-12-26 18:40:01.000000	N/A	Disabled
5244	680	svchost.exe	0xe38aba9e3080	9	-	0	False	2023-12-26 18:40:03.000000	N/A	Disabled
8224	680	svchost.exe	0xe38abbc66080	5	-	0	False	2023-12-26 18:40:04.000000	N/A	Disabled
8284	680	svchost.exe	0xe38aba9db080	4	-	0	False	2023-12-26 18:40:05.000000	N/A	Disabled
8396	680	svchost.exe	0xe38abbc6b080	2	-	0	False	2023-12-26 18:40:07.000000	N/A	Disabled
8440	680	svchost.exe	0xe38abbdd8080	4	-	0	False	2023-12-26 18:40:08.000000	N/A	Disabled
8588	680	svchost.exe	0xe38aba9e2080	8	-	0	False	2023-12-26 18:40:09.000000	N/A	Disabled
1804	804	PhoneExperienc	0xe38abb805080	17	-	1	False	2023-12-26 18:40:37.000000	N/A	Disabled
8412	804	RuntimeBroker.	0xe38ab3621340	2	-	1	False	2023-12-26 18:40:41.000000	N/A	Disabled
5980	680	svchost.exe	0xe38ab9c55080	3	-	0	False	2023-12-26 18:41:21.000000	N/A	Disabled
4416	680	svchost.exe	0xe38abbce0080	0	-	0	False	2023-12-26 18:41:23.000000	2023-12-26 18:41:26.000000	Disabled
8924	804	RuntimeBroker.	0xe38ab491f080	7	-	1	False	2023-12-26 18:42:49.000000	N/A	Disabled
1900	804	UserOOBEBroker	0xe38aba3dc080	4	-	1	False	2023-12-26 18:48:42.000000	N/A	Disabled
2744	804	SystemSettings	0xe38abb576080	18	-	1	False	2023-12-26 18:53:03.000000	N/A	Disabled
7172	804	ApplicationFra	0xe38abb74f080	4	-	1	False	2023-12-26 18:53:03.000000	N/A	Disabled
0	0		0xe38ab47f6080	0	-	N/A	False	N/A	N/A	Disabled

El primer comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: ***“python vol.py -f C:\Herramientas\windows_ram.mem windows.pslist.PsList”***

El comando windows.pslist.PsList se utiliza para extraer y mostrar información sobre los procesos que estaban en ejecución en un sistema Windows en el momento en que se creó el volcado de memoria. Estos procesos pueden incluir aplicaciones y servicios que estaban activos en ese momento. Este análisis puede ser útil para investigar incidentes de seguridad, identificar procesos maliciosos o comprender la actividad del sistema en un momento específico.

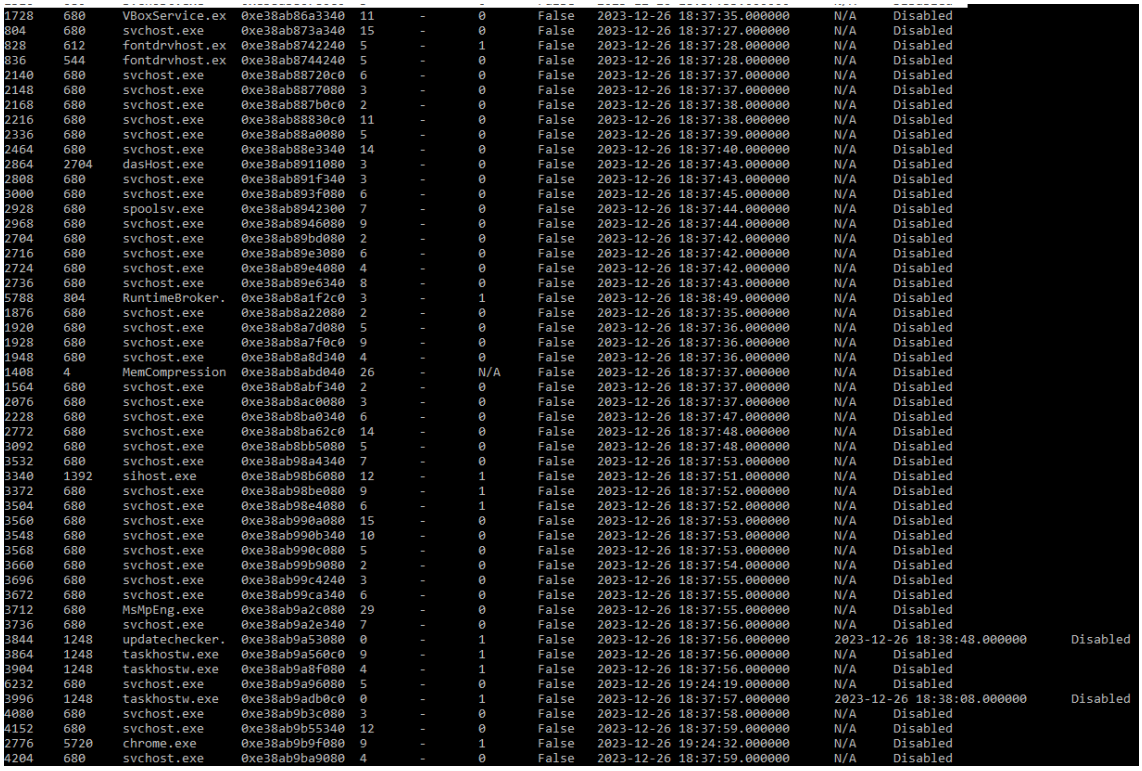
Una de las cosas que podemos destacar de este análisis es la siguiente información ***“6896 3856 GoogleCrashHan 0xe38ab4c7a080 5 - 0 True 2023-12-26 18:39:23.000000 N/A Disabled”***

Que es un comando que es un ping a Google.com que habíamos lanzado en el momento de la adquisición.

2.2 Windows.psscan.PsScan

```
C:\Herramientas\volatility3-2.4.0\volatility3-2.4.0>python vol.py -f C:\Herramientas\windows_ram.mem windows.psscan.PsScan
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File outp

4       0       System  0xe38ab1e83040  127     -       N/A     False   2023-12-26 18:37:01.000000      N/A     Disabled
1584    680     svchost.exe     0xe38ab1e86080  6       -       0       False   2023-12-26 18:37:33.000000      N/A     Disabled
92      4       Registry        0xe38ab1fba040  4       -       N/A     False   2023-12-26 18:36:34.000000      N/A     Disabled
8412    804     RuntimeBroker.  0xe38ab3621340  2       -       1       False   2023-12-26 18:40:41.000000      N/A     Disabled
5696    680     svchost.exe     0xe38ab38d5080  3       -       0       False   2023-12-26 18:39:59.000000      N/A     Disabled
1084    804     RuntimeBroker.  0xe38ab38d6240  10      -       1       False   2023-12-26 18:38:56.000000      N/A     Disabled
348     4       smss.exe        0xe38ab3e7f040  2       -       N/A     False   2023-12-26 18:37:01.000000      N/A     Disabled
1688    680     svchost.exe     0xe38ab454d080  8       -       0       False   2023-12-26 18:37:34.000000      N/A     Disabled
612     536     winlogon.exe    0xe38ab4555080  6       -       1       False   2023-12-26 18:37:24.000000      N/A     Disabled
7480    680     svchost.exe     0xe38ab462d2c0  2       -       1       False   2023-12-26 18:39:53.000000      N/A     Disabled
2092    612     dwm.exe 0xe38ab4855080  22      -       1       False   2023-12-26 19:28:47.000000      N/A     Disabled
5972    804     MoUsoCoreWorke  0xe38ab48d3080  7       -       0       False   2023-12-26 18:38:52.000000      N/A     Disabled
8924    804     RuntimeBroker.  0xe38ab491f080  7       -       1       False   2023-12-26 18:42:49.000000      N/A     Disabled
6584    680     SecurityHealth  0xe38ab49ba080  9       -       0       False   2023-12-26 18:39:16.000000      N/A     Disabled
6612    768     VBoxTray.exe    0xe38ab49bb080  11      -       1       False   2023-12-26 18:39:17.000000      N/A     Disabled
6552    768     SecurityHealth  0xe38ab49be080  3       -       1       False   2023-12-26 18:39:16.000000      N/A     Disabled
544     448     wininit.exe     0xe38ab4a80080  1       -       0       False   2023-12-26 18:37:24.000000      N/A     Disabled
680     544     services.exe    0xe38ab4a83140  10      -       0       False   2023-12-26 18:37:25.000000      N/A     Disabled
552     536     csrss.exe       0xe38ab4a85140  12      -       1       False   2023-12-26 18:37:24.000000      N/A     Disabled
2356    680     SearchIndexer.  0xe38ab4aae340  19      -       0       False   2023-12-26 18:38:57.000000      N/A     Disabled
4184    680     NisSrv.exe      0xe38ab4ab62c0  4       -       0       False   2023-12-26 18:38:59.000000      N/A     Disabled
928     680     svchost.exe     0xe38ab4c09080  18      -       0       False   2023-12-26 18:37:28.000000      N/A     Disabled
6896    3856    GoogleCrashHan  0xe38ab4c7a080  5       -       0       True    2023-12-26 18:39:23.000000      N/A     Disabled
3064    804     dllhost.exe     0xe38ab4c7b080  12      -       1       False   2023-12-26 19:19:43.000000      N/A     Disabled
6800    768     msedge.exe      0xe38ab4c7e080  51      -       1       False   2023-12-26 18:39:19.000000      N/A     Disabled
696     544     lsass.exe       0xe38ab4ca4080  12      -       0       False   2023-12-26 18:37:25.000000      N/A     Disabled
6188    680     svchost.exe     0xe38ab4ef3080  8       -       0       False   2023-12-26 19:28:35.000000      N/A     Disabled
460     448     csrss.exe       0xe38ab4f0b080  11      -       0       False   2023-12-26 18:37:22.000000      N/A     Disabled
1964    680     svchost.exe     0xe38ab4fe30c0  10      -       0       False   2023-12-26 18:37:36.000000      N/A     Disabled
980     680     svchost.exe     0xe38ab8224340  6       -       0       False   2023-12-26 18:37:28.000000      N/A     Disabled
5888    680     svchost.exe     0xe38ab842c340  9       -       0       False   2023-12-26 18:38:51.000000      N/A     Disabled
2584    680     svchost.exe     0xe38ab84a3080  11      -       0       False   2023-12-26 18:37:41.000000      N/A     Disabled
720     680     svchost.exe     0xe38ab851d340  6       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1032    680     svchost.exe     0xe38ab85230c0  4       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1056    680     svchost.exe     0xe38ab852a080  2       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1040    680     svchost.exe     0xe38ab852b080  3       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1108    680     svchost.exe     0xe38ab854a080  4       -       0       False   2023-12-26 18:37:30.000000      N/A     Disabled
1228    680     svchost.exe     0xe38ab8581080  8       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1240    680     svchost.exe     0xe38ab8584340  5       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1248    680     svchost.exe     0xe38ab8587340  12      -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1332    680     svchost.exe     0xe38ab85b9080  5       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1340    680     svchost.exe     0xe38ab85bc0c0  5       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1392    680     svchost.exe     0xe38ab8621340  7       -       0       False   2023-12-26 18:37:31.000000      N/A     Disabled
1444    680     svchost.exe     0xe38ab8627080  7       -       0       False   2023-12-26 18:37:32.000000      N/A     Disabled
1516    680     svchost.exe     0xe38ab86780c0  3       -       0       False   2023-12-26 18:37:33.000000      N/A     Disabled
```



1728	680	VBoxService.ex	0xe38ab86a3340	11	-	0	False	2023-12-26 18:37:35.000000	N/A	Disabled
804	680	svchost.exe	0xe38ab873a340	15	-	0	False	2023-12-26 18:37:27.000000	N/A	Disabled
828	612	fontdrvhost.ex	0xe38ab8742240	5	-	1	False	2023-12-26 18:37:28.000000	N/A	Disabled
836	544	fontdrvhost.ex	0xe38ab8744240	5	-	0	False	2023-12-26 18:37:28.000000	N/A	Disabled
2140	680	svchost.exe	0xe38ab88720c0	6	-	0	False	2023-12-26 18:37:37.000000	N/A	Disabled
2148	680	svchost.exe	0xe38ab8877080	3	-	0	False	2023-12-26 18:37:37.000000	N/A	Disabled
2168	680	svchost.exe	0xe38ab887b0c0	2	-	0	False	2023-12-26 18:37:38.000000	N/A	Disabled
2216	680	svchost.exe	0xe38ab88830c0	11	-	0	False	2023-12-26 18:37:38.000000	N/A	Disabled
2336	680	svchost.exe	0xe38ab88a0080	5	-	0	False	2023-12-26 18:37:39.000000	N/A	Disabled
2464	680	svchost.exe	0xe38ab88e3340	14	-	0	False	2023-12-26 18:37:40.000000	N/A	Disabled
2864	2704	dasHost.exe	0xe38ab8911080	3	-	0	False	2023-12-26 18:37:43.000000	N/A	Disabled
2808	680	svchost.exe	0xe38ab891f340	3	-	0	False	2023-12-26 18:37:43.000000	N/A	Disabled
3000	680	svchost.exe	0xe38ab893f080	6	-	0	False	2023-12-26 18:37:45.000000	N/A	Disabled
2928	680	spoolsv.exe	0xe38ab8942300	7	-	0	False	2023-12-26 18:37:44.000000	N/A	Disabled
2968	680	svchost.exe	0xe38ab8946080	9	-	0	False	2023-12-26 18:37:44.000000	N/A	Disabled
2704	680	svchost.exe	0xe38ab89bd080	2	-	0	False	2023-12-26 18:37:42.000000	N/A	Disabled
2716	680	svchost.exe	0xe38ab89e3080	6	-	0	False	2023-12-26 18:37:42.000000	N/A	Disabled
2724	680	svchost.exe	0xe38ab89e4080	4	-	0	False	2023-12-26 18:37:42.000000	N/A	Disabled
2736	680	svchost.exe	0xe38ab89e6340	8	-	0	False	2023-12-26 18:37:43.000000	N/A	Disabled
5788	804	RuntimeBroker.	0xe38ab8a1f2c0	3	-	1	False	2023-12-26 18:38:49.000000	N/A	Disabled
1876	680	svchost.exe	0xe38ab8a22080	2	-	0	False	2023-12-26 18:37:35.000000	N/A	Disabled
1920	680	svchost.exe	0xe38ab8a7d080	5	-	0	False	2023-12-26 18:37:36.000000	N/A	Disabled
1928	680	svchost.exe	0xe38ab8a7f0c0	9	-	0	False	2023-12-26 18:37:36.000000	N/A	Disabled
1948	680	svchost.exe	0xe38ab8a8d340	4	-	0	False	2023-12-26 18:37:36.000000	N/A	Disabled
1408	4	MemCompression	0xe38ab8abd040	26	-	N/A	False	2023-12-26 18:37:37.000000	N/A	Disabled
1564	680	svchost.exe	0xe38ab8abf340	2	-	0	False	2023-12-26 18:37:37.000000	N/A	Disabled
2076	680	svchost.exe	0xe38ab8ac0080	3	-	0	False	2023-12-26 18:37:37.000000	N/A	Disabled
2228	680	svchost.exe	0xe38ab8ba0340	6	-	0	False	2023-12-26 18:37:47.000000	N/A	Disabled
2772	680	svchost.exe	0xe38ab8ba62c0	14	-	0	False	2023-12-26 18:37:48.000000	N/A	Disabled
3092	680	svchost.exe	0xe38ab8bb5080	5	-	0	False	2023-12-26 18:37:48.000000	N/A	Disabled
3532	680	svchost.exe	0xe38ab98a4340	7	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3340	1392	sihost.exe	0xe38ab98b6080	12	-	1	False	2023-12-26 18:37:51.000000	N/A	Disabled
3372	680	svchost.exe	0xe38ab98be080	9	-	1	False	2023-12-26 18:37:52.000000	N/A	Disabled
3504	680	svchost.exe	0xe38ab98e4080	6	-	1	False	2023-12-26 18:37:52.000000	N/A	Disabled
3560	680	svchost.exe	0xe38ab990a080	15	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3548	680	svchost.exe	0xe38ab990b340	10	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3568	680	svchost.exe	0xe38ab990c080	5	-	0	False	2023-12-26 18:37:53.000000	N/A	Disabled
3660	680	svchost.exe	0xe38ab99b9080	2	-	0	False	2023-12-26 18:37:54.000000	N/A	Disabled
3696	680	svchost.exe	0xe38ab99c4240	3	-	0	False	2023-12-26 18:37:55.000000	N/A	Disabled
3672	680	svchost.exe	0xe38ab99ca340	6	-	0	False	2023-12-26 18:37:55.000000	N/A	Disabled
3712	680	MsMpEng.exe	0xe38ab9a2c080	29	-	0	False	2023-12-26 18:37:55.000000	N/A	Disabled
3736	680	svchost.exe	0xe38ab9a2e340	7	-	0	False	2023-12-26 18:37:56.000000	N/A	Disabled
3844	1248	updatechecker.	0xe38ab9a53080	0	-	1	False	2023-12-26 18:37:56.000000	2023-12-26 18:38:48.000000	Disabled
3864	1248	taskhostw.exe	0xe38ab9a560c0	9	-	1	False	2023-12-26 18:37:56.000000	N/A	Disabled
3904	1248	taskhostw.exe	0xe38ab9a8f080	4	-	1	False	2023-12-26 18:37:56.000000	N/A	Disabled
6232	680	svchost.exe	0xe38ab9a96080	5	-	0	False	2023-12-26 19:24:19.000000	N/A	Disabled
3996	1248	taskhostw.exe	0xe38ab9adb0c0	0	-	1	False	2023-12-26 18:37:57.000000	2023-12-26 18:38:08.000000	Disabled
4080	680	svchost.exe	0xe38ab9b3c080	3	-	0	False	2023-12-26 18:37:58.000000	N/A	Disabled
4152	680	svchost.exe	0xe38ab9b55340	12	-	0	False	2023-12-26 18:37:59.000000	N/A	Disabled
2776	5720	chrome.exe	0xe38ab9b9f080	9	-	1	False	2023-12-26 19:24:32.000000	N/A	Disabled
4204	680	svchost.exe	0xe38ab9ba9080	4	-	0	False	2023-12-26 18:37:59.000000	N/A	Disabled

El segundo comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: ***"python vol.py -f C:\Herramientas\windows_ram.mem windows.psscan.PsScan"***

Este comando está diseñado para escanear la memoria en busca de información sobre procesos.

Es útil para obtener una vista más detallada y extensa de la información del proceso en comparación con el comando pslist. Puedes usarse para realizar un análisis más profundo de los procesos presentes en un volcado de memoria y obtener información adicional, como detalles de seguridad y tiempo de CPU utilizado.

"7796 5720 chrome.exe 0xe38abb782080 15 - 1 False 2023-12-26 19:24:33.000000 N/A Disabled"

"7860 768 notepad++.exe 0xe38abb785080 5 - 1 False 2023-12-26 19:24:51.000000 N/A Disabled"

Podemos destacar estos dos procesos que había activado en el sistema en el momento en el que creé el volcado de sistema.

2.3 Windows.pstree.PsTree

```
C:\Herramientas\volatility3-2.4.0\volatility3-2.4.0>python vol.py -f C:\Herramientas\windows_ram.mem windows.pstree.PsTree
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xe38ab1e83040  127     -       N/A     False   2023-12-26 18:37:01.000000      N/A
* 1408  4       MemCompression  0xe38ab8abd040  26      -       N/A     False   2023-12-26 18:37:37.000000      N/A
* 92    4       Registry        0xe38ab1fba040  4       -       N/A     False   2023-12-26 18:36:34.000000      N/A
* 348   4       smss.exe        0xe38ab3e7f040  2       -       N/A     False   2023-12-26 18:37:01.000000      N/A
460     448     csrss.exe       0xe38ab4f0b080  11      -       0       False   2023-12-26 18:37:22.000000      N/A
544     448     wininit.exe     0xe38ab4a80080  1       -       0       False   2023-12-26 18:37:24.000000      N/A
* 680   544     services.exe    0xe38ab4a83140  10      -       0       False   2023-12-26 18:37:25.000000      N/A
** 1032 680     svchost.exe     0xe38ab85230c0  4       -       0       False   2023-12-26 18:37:30.000000      N/A
** 1040 680     svchost.exe     0xe38ab852b080  3       -       0       False   2023-12-26 18:37:30.000000      N/A
** 3092 680     svchost.exe     0xe38ab8bb5080  5       -       0       False   2023-12-26 18:37:48.000000      N/A
** 2584 680     svchost.exe     0xe38ab84a3080  11      -       0       False   2023-12-26 18:37:41.000000      N/A
** 1564 680     svchost.exe     0xe38ab8abf340  2       -       0       False   2023-12-26 18:37:37.000000      N/A
** 2076 680     svchost.exe     0xe38ab8ac0080  3       -       0       False   2023-12-26 18:37:37.000000      N/A
** 1056 680     svchost.exe     0xe38ab852a080  2       -       0       False   2023-12-26 18:37:30.000000      N/A
** 8224 680     svchost.exe     0xe38abbc66080  5       -       0       False   2023-12-26 18:40:04.000000      N/A
** 1584 680     svchost.exe     0xe38ab1e86080  6       -       0       False   2023-12-26 18:37:33.000000      N/A
** 4152 680     svchost.exe     0xe38ab9b55340  12      -       0       False   2023-12-26 18:37:59.000000      N/A
** 5696 680     svchost.exe     0xe38ab38d5080  3       -       0       False   2023-12-26 18:39:59.000000      N/A
** 3660 680     svchost.exe     0xe38ab99b9080  2       -       0       False   2023-12-26 18:37:54.000000      N/A
** 1108 680     svchost.exe     0xe38ab854a080  4       -       0       False   2023-12-26 18:37:30.000000      N/A
** 3672 680     svchost.exe     0xe38ab99ca340  6       -       0       False   2023-12-26 18:37:55.000000      N/A
** 4184 680     NisSrv.exe      0xe38ab4ab62c0  4       -       0       False   2023-12-26 18:38:59.000000      N/A
** 2140 680     svchost.exe     0xe38ab88720c0  6       -       0       False   2023-12-26 18:37:37.000000      N/A
** 4188 680     svchost.exe     0xe38aba3f4080  5       -       0       False   2023-12-26 18:39:04.000000      N/A
** 8284 680     svchost.exe     0xe38aba9db080  4       -       0       False   2023-12-26 18:40:05.000000      N/A
** 2148 680     svchost.exe     0xe38ab8877080  3       -       0       False   2023-12-26 18:37:37.000000      N/A
** 4204 680     svchost.exe     0xe38ab9ba9080  4       -       0       False   2023-12-26 18:37:59.000000      N/A
*** 4376       4204    ctfmon.exe      0xe38ab9c350c0  10      -       1       False   2023-12-26 18:38:01.000000      N/A
** 3696 680     svchost.exe     0xe38ab99c4240  3       -       0       False   2023-12-26 18:37:55.000000      N/A
** 2168 680     svchost.exe     0xe38ab887b0c0  2       -       0       False   2023-12-26 18:37:38.000000      N/A
** 5244 680     svchost.exe     0xe38aba9e3080  9       -       0       False   2023-12-26 18:40:03.000000      N/A
** 3712 680     MsMpEng.exe     0xe38ab9a2c080  29      -       0       False   2023-12-26 18:37:55.000000      N/A
** 2704 680     svchost.exe     0xe38ab89bd080  2       -       0       False   2023-12-26 18:37:42.000000      N/A
*** 2864       2704    dasHost.exe     0xe38ab8911080  3       -       0       False   2023-12-26 18:37:43.000000      N/A
** 1688 680     svchost.exe     0xe38ab454d080  8       -       0       False   2023-12-26 18:37:34.000000      N/A
** 3736 680     svchost.exe     0xe38ab9a2e340  7       -       0       False   2023-12-26 18:37:56.000000      N/A
** 2716 680     svchost.exe     0xe38ab89e3080  6       -       0       False   2023-12-26 18:37:42.000000      N/A
** 2724 680     svchost.exe     0xe38ab89e4080  4       -       0       False   2023-12-26 18:37:42.000000      N/A
** 2216 680     svchost.exe     0xe38ab88830c0  11      -       0       False   2023-12-26 18:37:38.000000      N/A
** 2736 680     svchost.exe     0xe38ab89e6340  8       -       0       False   2023-12-26 18:37:43.000000      N/A
** 2228 680     svchost.exe     0xe38ab8ba0340  6       -       0       False   2023-12-26 18:37:47.000000      N/A
** 1728 680     VBoxService.ex  0xe38ab86a3340  11      -       0       False   2023-12-26 18:37:35.000000      N/A
** 4800 680     svchost.exe     0xe38ab9e4d340  6       -       0       False   2023-12-26 18:38:09.000000      N/A
** 1228 680     svchost.exe     0xe38ab8581080  8       -       0       False   2023-12-26 18:37:31.000000      N/A
** 8396 680     svchost.exe     0xe38abbc6b080  2       -       0       False   2023-12-26 18:40:07.000000      N/A
** 720  680     svchost.exe     0xe38ab851d340  6       -       0       False   2023-12-26 18:37:30.000000      N/A
** 2772 680     svchost.exe     0xe38ab8ba62c0  14      -       0       False   2023-12-26 18:37:48.000000      N/A
** 1240 680     svchost.exe     0xe38ab8584340  5       -       0       False   2023-12-26 18:37:31.000000      N/A
** 1248 680     svchost.exe     0xe38ab8587340  12      -       0       False   2023-12-26 18:37:31.000000      N/A
*** 3864       1248    taskhostw.exe   0xe38ab9a560c0  9       -       1       False   2023-12-26 18:37:56.000000      N/A
```

```
*** 3996       1248    taskhostw.exe   0xe38ab9adb0c0  0       -       1       False   2023-12-26 18:37:57.000000      2023-12-26 18:38:08.000000
*** 3904       1248    taskhostw.exe   0xe38ab9a8f080  4       -       1       False   2023-12-26 18:37:56.000000      N/A
*** 3844       1248    updatechecker.  0xe38ab9a53080  0       -       1       False   2023-12-26 18:37:56.000000      2023-12-26 18:38:48.000000
**** 5276      3844    updatechecker.  0xe38aba198080  15      -       1       False   2023-12-26 18:38:36.000000      N/A
** 2808 680     svchost.exe     0xe38ab891f340  3       -       0       False   2023-12-26 18:37:43.000000      N/A
** 8440 680     svchost.exe     0xe38abbdd8080  4       -       0       False   2023-12-26 18:40:08.000000      N/A
** 5888 680     svchost.exe     0xe38ab842c340  9       -       0       False   2023-12-26 18:38:51.000000      N/A
** 2336 680     svchost.exe     0xe38ab88a0080  5       -       0       False   2023-12-26 18:37:39.000000      N/A
** 804  680     svchost.exe     0xe38ab873a340  15      -       0       False   2023-12-26 18:37:27.000000      N/A
*** 5568       804     StartMenuExper  0xe38ab9cf3080  10      -       1       False   2023-12-26 18:38:45.000000      N/A
*** 8924       804     RuntimeBroker.  0xe38ab491f080  7       -       1       False   2023-12-26 18:42:49.000000      N/A
*** 7172       804     ApplicationFra  0xe38abb74f080  4       -       1       False   2023-12-26 18:53:03.000000      N/A
*** 1804       804     PhoneExperienc  0xe38abb805080  17      -       1       False   2023-12-26 18:40:37.000000      N/A
*** 1900       804     UserOOBEBroker  0xe38aba3dc080  4       -       1       False   2023-12-26 18:48:42.000000      N/A
*** 1084       804     RuntimeBroker.  0xe38ab38d6240  10      -       1       False   2023-12-26 18:38:56.000000      N/A
*** 2744       804     SystemSettings  0xe38abb576080  18      -       1       False   2023-12-26 18:53:03.000000      N/A
*** 8412       804     RuntimeBroker.  0xe38ab3621340  2       -       1       False   2023-12-26 18:40:41.000000      N/A
*** 5972       804     MoUsoCoreWorke  0xe38ab48d3080  7       -       0       False   2023-12-26 18:38:52.000000      N/A
*** 6072       804     SearchApp.exe   0xe38aba37a080  47      -       1       False   2023-12-26 18:39:27.000000      N/A
*** 5560       804     TextInputHost.  0xe38ab9d1e080  11      -       1       False   2023-12-26 18:38:45.000000      N/A
*** 5788       804     RuntimeBroker.  0xe38ab8a1f2c0  3       -       1       False   2023-12-26 18:38:49.000000      N/A
** 3372 680     svchost.exe     0xe38ab98be080  9       -       1       False   2023-12-26 18:37:52.000000      N/A
** 1332 680     svchost.exe     0xe38ab85b9080  5       -       0       False   2023-12-26 18:37:31.000000      N/A
** 2356 680     SearchIndexer.  0xe38ab4aae340  19      -       0       False   2023-12-26 18:38:57.000000      N/A
** 7480 680     svchost.exe     0xe38ab462d2c0  2       -       1       False   2023-12-26 18:39:53.000000      N/A
** 1340 680     svchost.exe     0xe38ab85bc0c0  5       -       0       False   2023-12-26 18:37:31.000000      N/A
** 4416 680     svchost.exe     0xe38abbce0080  0       -       0       False   2023-12-26 18:41:23.000000      2023-12-26 18:41:26.000000
** 1876 680     svchost.exe     0xe38ab8a22080  2       -       0       False   2023-12-26 18:37:35.000000      N/A
** 5980 680     svchost.exe     0xe38ab9c55080  3       -       0       False   2023-12-26 18:41:21.000000      N/A
** 4968 680     svchost.exe     0xe38ab9d1f080  0       -       0       False   2023-12-26 18:38:12.000000      2023-12-26 18:44:25.000000
** 1392 680     svchost.exe     0xe38ab8621340  7       -       0       False   2023-12-26 18:37:31.000000      N/A
*** 3340       1392    sihost.exe      0xe38ab98b6080  12      -       1       False   2023-12-26 18:37:51.000000      N/A
** 2928 680     spoolsv.exe     0xe38ab8942300  7       -       0       False   2023-12-26 18:37:44.000000      N/A
** 1920 680     svchost.exe     0xe38ab8a7d080  5       -       0       False   2023-12-26 18:37:36.000000      N/A
** 1928 680     svchost.exe     0xe38ab8a7f0c0  9       -       0       False   2023-12-26 18:37:36.000000      N/A
** 6028 680     SgrmBroker.exe  0xe38abbd6e080  7       -       0       False   2023-12-26 18:40:01.000000      N/A
** 8588 680     svchost.exe     0xe38aba9e2080  8       -       0       False   2023-12-26 18:40:09.000000      N/A
** 2968 680     svchost.exe     0xe38ab8946080  9       -       0       False   2023-12-26 18:37:44.000000      N/A
** 1948 680     svchost.exe     0xe38ab8a8d340  4       -       0       False   2023-12-26 18:37:36.000000      N/A
** 928  680     svchost.exe     0xe38ab4c09080  18      -       0       False   2023-12-26 18:37:28.000000      N/A
** 2464 680     svchost.exe     0xe38ab88e3340  14      -       0       False   2023-12-26 18:37:40.000000      N/A
** 1444 680     svchost.exe     0xe38ab8627080  7       -       0       False   2023-12-26 18:37:32.000000      N/A
** 1964 680     svchost.exe     0xe38ab4fe30c0  10      -       0       False   2023-12-26 18:37:36.000000      N/A
** 5036 680     svchost.exe     0xe38ab9f91080  8       -       1       False   2023-12-26 18:38:30.000000      N/A
** 3504 680     svchost.exe     0xe38ab98e4080  6       -       1       False   2023-12-26 18:37:52.000000      N/A
** 4528 680     svchost.exe     0xe38ab9cf2080  7       -       0       False   2023-12-26 18:38:04.000000      N/A
** 3000 680     svchost.exe     0xe38ab893f080  6       -       0       False   2023-12-26 18:37:45.000000      N/A
** 6584 680     SecurityHealth  0xe38ab49ba080  9       -       0       False   2023-12-26 18:39:16.000000      N/A
** 3532 680     svchost.exe     0xe38ab98a4340  7       -       0       False   2023-12-26 18:37:53.000000      N/A
** 980  680     svchost.exe     0xe38ab8224340  6       -       0       False   2023-12-26 18:37:28.000000      N/A
** 3548 680     svchost.exe     0xe38ab990b340  10      -       0       False   2023-12-26 18:37:53.000000      N/A
** 3560 680     svchost.exe     0xe38ab990a080  15      -       0       False   2023-12-26 18:37:53.000000      N/A
** 1516 680     svchost.exe     0xe38ab86780c0  3       -       0       False   2023-12-26 18:37:33.000000      N/A
** 3568 680     svchost.exe     0xe38ab990c080  5       -       0       False   2023-12-26 18:37:53.000000      N/A
```

```
** 4080 680     svchost.exe     0xe38ab9b3c080  3       -       0       False   2023-12-26 18:37:58.000000      N/A
* 836   544     fontdrvhost.ex  0xe38ab8744240  5       -       0       False   2023-12-26 18:37:28.000000      N/A
* 696   544     lsass.exe       0xe38ab4ca4080  12      -       0       False   2023-12-26 18:37:25.000000      N/A
552     536     csrss.exe       0xe38ab4a85140  12      -       1       False   2023-12-26 18:37:24.000000      N/A
612     536     winlogon.exe    0xe38ab4555080  6       -       1       False   2023-12-26 18:37:24.000000      N/A
* 1664  612     userinit.exe    0xe38ab9eb8080  0       -       1       False   2023-12-26 18:38:23.000000      2023-12-26 18:38:42.000000
** 768  1664    explorer.exe    0xe38ab9c1d080  55      -       1       False   2023-12-26 18:38:24.000000      N/A
*** 6552       768     SecurityHealth  0xe38ab49be080  3       -       1       False   2023-12-26 18:39:16.000000      N/A
*** 6612       768     VBoxTray.exe    0xe38ab49bb080  11      -       1       False   2023-12-26 18:39:17.000000      N/A
*** 6800       768     msedge.exe      0xe38ab4c7e080  51      -       1       False   2023-12-26 18:39:19.000000      N/A
**** 3616      6800    msedge.exe      0xe38abb7020c0  8       -       1       False   2023-12-26 18:39:26.000000      N/A
**** 6924      6800    msedge.exe      0xe38abb5c90c0  8       -       1       False   2023-12-26 18:39:24.000000      N/A
**** 6096      6800    msedge.exe      0xe38abb6f4300  17      -       1       False   2023-12-26 18:39:26.000000      N/A
**** 7156      6800    msedge.exe      0xe38abb5860c0  16      -       1       False   2023-12-26 18:39:25.000000      N/A
**** 7128      6800    msedge.exe      0xe38abb6ef0c0  15      -       1       False   2023-12-26 18:39:25.000000      N/A
**** 7192      6800    msedge.exe      0xe38aba9ce280  14      -       1       False   2023-12-26 18:39:28.000000      N/A
* 828   612     fontdrvhost.ex  0xe38ab8742240  5       -       1       False   2023-12-26 18:37:28.000000      N/A
6896    3856    GoogleCrashHan  0xe38ab4c7a080  5       -       0       True    2023-12-26 18:39:23.000000      N/A
7396    3856    GoogleCrashHan  0xe38abb7340c0  3       -       0       False   2023-12-26 18:39:30.000000      N/A
```

El tercer comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: ***"python vol.py -f C:\Herramientas\windows_ram.mem windows.pstree.PsTree"***

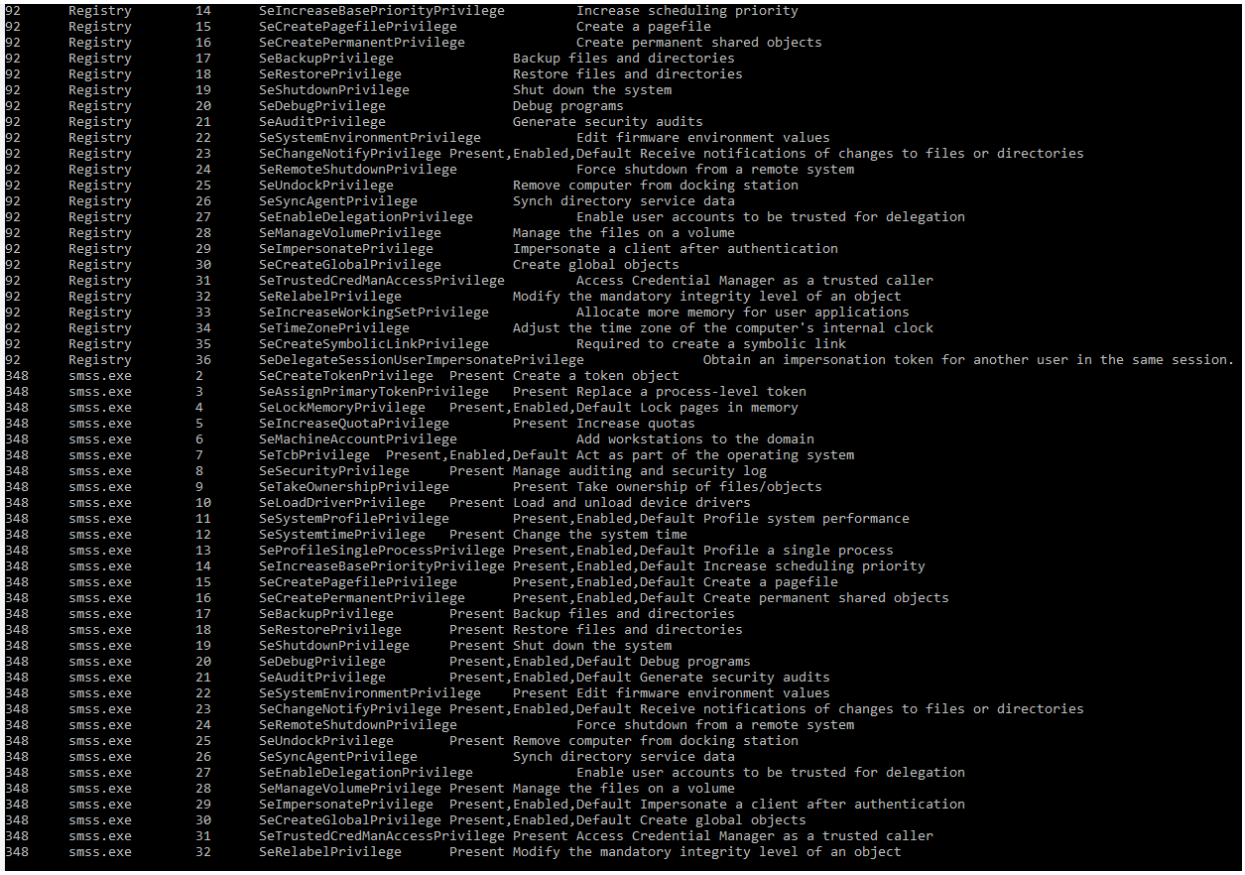
Este plugin se utiliza para visualizar la jerarquía de procesos en el sistema operativo Windows en forma de un árbol. Cada proceso se muestra como un nodo, y las relaciones de padre-hijo representan cómo se crearon los procesos.

Cuando se ejecuta este comando en un volcado de memoria de Windows, se obtiene una salida que muestra la relación jerárquica entre los procesos presentes en el sistema en el momento del volcado. Puede ser útil para entender cómo interactúan los diferentes procesos en el sistema.

2.4 Windows.privileges.Privs

```
C:\Herramientas\volatility3-2.4.0\volatility3-2.4.0>python vol.py -f C:\Herramientas\windows_ram.mem windows.privileges.Privs
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
PID     Process Value   Privilege       Attributes      Description

4       System  2       SeCreateTokenPrivilege  Present Create a token object
4       System  3       SeAssignPrimaryTokenPrivilege   Present Replace a process-level token
4       System  4       SeLockMemoryPrivilege   Present,Enabled,Default Lock pages in memory
4       System  5       SeIncreaseQuotaPrivilege        Present Increase quotas
4       System  6       SeMachineAccountPrivilege               Add workstations to the domain
4       System  7       SeTcbPrivilege  Present,Enabled,Default Act as part of the operating system
4       System  8       SeSecurityPrivilege     Present Manage auditing and security log
4       System  9       SeTakeOwnershipPrivilege        Present Take ownership of files/objects
4       System  10      SeLoadDriverPrivilege   Present Load and unload device drivers
4       System  11      SeSystemProfilePrivilege        Present,Enabled,Default Profile system performance
4       System  12      SeSystemtimePrivilege   Present Change the system time
4       System  13      SeProfileSingleProcessPrivilege Present,Enabled,Default Profile a single process
4       System  14      SeIncreaseBasePriorityPrivilege Present,Enabled,Default Increase scheduling priority
4       System  15      SeCreatePagefilePrivilege       Present,Enabled,Default Create a pagefile
4       System  16      SeCreatePermanentPrivilege      Present,Enabled,Default Create permanent shared objects
4       System  17      SeBackupPrivilege       Present Backup files and directories
4       System  18      SeRestorePrivilege      Present Restore files and directories
4       System  19      SeShutdownPrivilege     Present Shut down the system
4       System  20      SeDebugPrivilege        Present,Enabled,Default Debug programs
4       System  21      SeAuditPrivilege        Present,Enabled,Default Generate security audits
4       System  22      SeSystemEnvironmentPrivilege    Present Edit firmware environment values
4       System  23      SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files or directories
4       System  24      SeRemoteShutdownPrivilege               Force shutdown from a remote system
4       System  25      SeUndockPrivilege       Present Remove computer from docking station
4       System  26      SeSyncAgentPrivilege            Synch directory service data
4       System  27      SeEnableDelegationPrivilege             Enable user accounts to be trusted for delegation
4       System  28      SeManageVolumePrivilege Present Manage the files on a volume
4       System  29      SeImpersonatePrivilege  Present,Enabled,Default Impersonate a client after authentication
4       System  30      SeCreateGlobalPrivilege Present,Enabled,Default Create global objects
4       System  31      SeTrustedCredManAccessPrivilege Present Access Credential Manager as a trusted caller
4       System  32      SeRelabelPrivilege      Present Modify the mandatory integrity level of an object
4       System  33      SeIncreaseWorkingSetPrivilege   Present,Enabled,Default Allocate more memory for user applications
4       System  34      SeTimeZonePrivilege     Present,Enabled,Default Adjust the time zone of the computer's internal clock
4       System  35      SeCreateSymbolicLinkPrivilege   Present,Enabled,Default Required to create a symbolic link
4       System  36      SeDelegateSessionUserImpersonatePrivilege       Present,Enabled,Default Obtain an impersonation token for another user in the same session.
92      Registry        2       SeCreateTokenPrivilege          Create a token object
92      Registry        3       SeAssignPrimaryTokenPrivilege           Replace a process-level token
92      Registry        4       SeLockMemoryPrivilege           Lock pages in memory
92      Registry        5       SeIncreaseQuotaPrivilege                Increase quotas
92      Registry        6       SeMachineAccountPrivilege               Add workstations to the domain
92      Registry        7       SeTcbPrivilege          Act as part of the operating system
92      Registry        8       SeSecurityPrivilege             Manage auditing and security log
92      Registry        9       SeTakeOwnershipPrivilege                Take ownership of files/objects
92      Registry        10      SeLoadDriverPrivilege           Load and unload device drivers
92      Registry        11      SeSystemProfilePrivilege                Profile system performance
92      Registry        12      SeSystemtimePrivilege           Change the system time
92      Registry        13      SeProfileSingleProcessPrivilege         Profile a single process
```



```
92      Registry        14      SeIncreaseBasePriorityPrivilege         Increase scheduling priority
92      Registry        15      SeCreatePagefilePrivilege               Create a pagefile
92      Registry        16      SeCreatePermanentPrivilege              Create permanent shared objects
92      Registry        17      SeBackupPrivilege               Backup files and directories
92      Registry        18      SeRestorePrivilege              Restore files and directories
92      Registry        19      SeShutdownPrivilege             Shut down the system
92      Registry        20      SeDebugPrivilege                Debug programs
92      Registry        21      SeAuditPrivilege                Generate security audits
92      Registry        22      SeSystemEnvironmentPrivilege            Edit firmware environment values
92      Registry        23      SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files or directories
92      Registry        24      SeRemoteShutdownPrivilege               Force shutdown from a remote system
92      Registry        25      SeUndockPrivilege               Remove computer from docking station
92      Registry        26      SeSyncAgentPrivilege            Synch directory service data
92      Registry        27      SeEnableDelegationPrivilege             Enable user accounts to be trusted for delegation
92      Registry        28      SeManageVolumePrivilege         Manage the files on a volume
92      Registry        29      SeImpersonatePrivilege          Impersonate a client after authentication
92      Registry        30      SeCreateGlobalPrivilege         Create global objects
92      Registry        31      SeTrustedCredManAccessPrivilege         Access Credential Manager as a trusted caller
92      Registry        32      SeRelabelPrivilege              Modify the mandatory integrity level of an object
92      Registry        33      SeIncreaseWorkingSetPrivilege           Allocate more memory for user applications
92      Registry        34      SeTimeZonePrivilege             Adjust the time zone of the computer's internal clock
92      Registry        35      SeCreateSymbolicLinkPrivilege           Required to create a symbolic link
92      Registry        36      SeDelegateSessionUserImpersonatePrivilege               Obtain an impersonation token for another user in the same session.
348     smss.exe        2       SeCreateTokenPrivilege  Present Create a token object
348     smss.exe        3       SeAssignPrimaryTokenPrivilege   Present Replace a process-level token
348     smss.exe        4       SeLockMemoryPrivilege   Present,Enabled,Default Lock pages in memory
348     smss.exe        5       SeIncreaseQuotaPrivilege        Present Increase quotas
348     smss.exe        6       SeMachineAccountPrivilege               Add workstations to the domain
348     smss.exe        7       SeTcbPrivilege  Present,Enabled,Default Act as part of the operating system
348     smss.exe        8       SeSecurityPrivilege     Present Manage auditing and security log
348     smss.exe        9       SeTakeOwnershipPrivilege        Present Take ownership of files/objects
348     smss.exe        10      SeLoadDriverPrivilege   Present Load and unload device drivers
348     smss.exe        11      SeSystemProfilePrivilege        Present,Enabled,Default Profile system performance
348     smss.exe        12      SeSystemtimePrivilege   Present Change the system time
348     smss.exe        13      SeProfileSingleProcessPrivilege Present,Enabled,Default Profile a single process
348     smss.exe        14      SeIncreaseBasePriorityPrivilege Present,Enabled,Default Increase scheduling priority
348     smss.exe        15      SeCreatePagefilePrivilege       Present,Enabled,Default Create a pagefile
348     smss.exe        16      SeCreatePermanentPrivilege      Present,Enabled,Default Create permanent shared objects
348     smss.exe        17      SeBackupPrivilege       Present Backup files and directories
348     smss.exe        18      SeRestorePrivilege      Present Restore files and directories
348     smss.exe        19      SeShutdownPrivilege     Present Shut down the system
348     smss.exe        20      SeDebugPrivilege        Present,Enabled,Default Debug programs
348     smss.exe        21      SeAuditPrivilege        Present,Enabled,Default Generate security audits
348     smss.exe        22      SeSystemEnvironmentPrivilege    Present Edit firmware environment values
348     smss.exe        23      SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files or directories
348     smss.exe        24      SeRemoteShutdownPrivilege               Force shutdown from a remote system
348     smss.exe        25      SeUndockPrivilege       Present Remove computer from docking station
348     smss.exe        26      SeSyncAgentPrivilege            Synch directory service data
348     smss.exe        27      SeEnableDelegationPrivilege             Enable user accounts to be trusted for delegation
348     smss.exe        28      SeManageVolumePrivilege Present Manage the files on a volume
348     smss.exe        29      SeImpersonatePrivilege  Present,Enabled,Default Impersonate a client after authentication
348     smss.exe        30      SeCreateGlobalPrivilege Present,Enabled,Default Create global objects
348     smss.exe        31      SeTrustedCredManAccessPrivilege Present Access Credential Manager as a trusted caller
348     smss.exe        32      SeRelabelPrivilege      Present Modify the mandatory integrity level of an object
```

El cuarto comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: ***"python vol.py -f C:\Herramientas\windows_ram.mem windows.privileges.Privs"***

Este plugin se utiliza para listar los privilegios asignados a cada proceso en el sistema operativo Windows en el momento en que se creó el volcado de memoria.

Cuando ejecutas este comando, obtendrás una salida que muestra información sobre los procesos y los privilegios que tienen asignados. Los privilegios son derechos especiales que un proceso puede tener y que permiten realizar acciones específicas en el sistema.

Por ejemplo, la salida puede incluir información sobre procesos que tienen privilegios elevados, como el derecho a realizar acciones críticas en el sistema. Esto puede ser útil para la investigación de incidentes de seguridad y para comprender la configuración de seguridad del sistema en el momento del volcado de memoria.

En el pantallazo solo se muestra algunos pocos de la lista ya que el proceso era muy extenso.